(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3000968号
(P3000968)
(45)発行日　平成12年１月17日(2000.1.17)　(24)登録日　平成11年11月12日(1999.11.12)

(51)Int.Cl.⁷	識別記号	FI	
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/20	Ｄ
12/46		11/00	３１０Ｃ

請求項の数２(全 16 頁)

(21)出願番号　特願平9－183665
(22)出願日　平成９年７月９日(1997.7.9)
(65)公開番号　特開平11－32047
(43)公開日　平成11年２月２日(1999.2.2)
審査請求日　平成９年７月９日(1997.7.9)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　森　直樹
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100083987
弁理士　山内　梅雄

審査官　江嶋　清仁

(56)参考文献　1997信学総大Ｂ－７－124
信学論（Ｂ－１）ＶＯＬ．Ｊ80－Ｂ－１，ＮＯ．６，Ｐ．366－373

(58)調査した分野(Int.Cl.⁷，ＤＢ名)
H04L　12/28
H04L　12/46

(54)【発明の名称】　パケットフィルタリングシステム

1

(57)【特許請求の範囲】
【請求項１】　非同期転送モードのＡＴＭネットワーク上に構築したマルチプロトコルの転送のためのＭＰＯＡネットワークで、送信側ＭＰＯＡクライアントがアドレス解決手順を起動し、受信した受信ＩＰアドレスから出口側のＭＰＯＡ方式のネットワーク内のクライアントである出口側ＭＰＯＡクライアントのＡＴＭアドレスを獲得するようにした通信システムにおいて、
アドレス解決要求メッセージを受信してこのメッセージ内の送受信ＩＰアドレスとＴＣＰまたはＵＤＰポート番号をそれぞれ読み込んでこれらをフィルタ用の情報としてのセット情報として、通常のデータ転送のために設定されたフィルタリングの基準に応じてアドレス解決要求に応じるか否かを判定する判定手段と、この判定手段の判定の結果としてアドレス解決要求に応じる場合にはア

2

ドレス解決手順を進行させ、アドレス解決要求に応じない場合にはアドレス解決を中止することで、複数のＭＰＯＡサーバ上のフィルタリング基準のすべてに適合するセット情報のパケットに対してのみアドレス解決の結果を返信する返信手段を備えたＭＰＯＡサーバと、
アドレス解決要求メッセージ内に、これから設定するショートカット仮想チャネル・コネクションとしてのショートカットＶＣＣを通して送信するパケットの前記セット情報を挿入する挿入手段と、アドレス解決要求時に前記セット情報のうちアドレス解決が中止されずに完了したもののみを記憶する第１の記憶手段と、パケット送信時にこの第１の記憶手段に記憶した内容と一致するＩＰパケットのみをショートカットＶＣＣに送信する送信手段と、前記アドレス解決要求時に、前記ＭＰＯＡサーバから通知されたショートカットＶＣＣを通して送信され

てくるパケットの前記セット情報を記憶する第２の記憶手段と、パケット受信時にこの第２の記憶手段に記憶したセット情報と一致するＩＰパケットのみをショートカットＶＣＣから受けて、これ以外のＩＰパケットは廃棄するパケットフィルタリング手段とを備えたＭＰＯＡクライアントとを具備することを特徴とするパケットフィルタリングシステム。

【請求項２】　ＡＴＭインタフェースと他のネットワークインタフェースを持ったデバイスとしてのエッジデバイスやＡＴＭ端末がトランスポート・コントロール・プロトコル／ユーザ・データグラム・プロトコルとしてのＴＣＰ／ＵＤＰヘッダとＩＰヘッダを読むことで、前記セット情報によるパケットフィルタリングを実現することを特徴とする請求項１記載のパケットフィルタリングシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は非同期転送ネットワークを使用したＴＣＰ／ＩＰプロトコルによるインターネットに係わり、特にインターネットでセキュリティ機能を実現するために許可されたデータのみを通過させるためのパケットフィルタリングシステムに関する。

【０００２】

【従来の技術】ネットワーク層にＩＰ（Internet Protocol）を使用し、トランスポート層にＴＣＰ（Transport Control Protocol）を使用してＴＣＰ／ＩＰ（Transport Control Protocol／Internet Protocol）ネットワークを相互接続するために、ルータが従来から使用されている。ルータは複数のネットワークインタフェースを有しており、ネットワーク層までの処理を終端する。また、トランスポート層の処理も一部行うことがある。

【０００３】このルータの機能の１つとして、パケットの選択的通過すなわちフィルタリングによる通信のセキュリティの確保がある。今、あるネットワークの外部に存在するＩＰノードが、そのネットワークの内部に存在するＩＰノードと通信を行うものとする。このとき、パケットはそのネットワークの出入口に配置されたルータを経由する。ルータは、その通過しようとするパケット内のネットワーク層とトランスポート層のヘッダを読んで転送処理を行う。このため、通過してよいＩＰパケットの送信ノードおよび受信ノードのＩＰアドレスとＴＣＰ／ＵＤＰ（Transport Control Protocol／User Datagram Protocol）のポート番号（セット情報）を予め設定しておいて、これと照合して該当しないパケットを廃棄するように設定しておけば、アクセスを制限することができる。すなわち、ネットワーク内部のＩＰノードを外部からアクセスできないようにしたり、トランスポート層の特定のポートへのアクセスを禁止したりすることが可能になる。これらは、それぞれ、ネットワーク層レベルにおけるパケットフィルタリングあるいはトランスポート層レベルのパケットフィルタリングと呼ばれており、通信のセキュリティを高めることに有効である。

【０００４】一方、ネットワークの高速化を図るために、ルータの変わりに高速なＡＴＭ（Asynchronous Transfer Mode：非同期転送モード）交換機を使用してＴＣＰ／ＩＰネットワークを構築するための技術が開発されている。例えば、ＯＳＩ（OpenSystems Interconnection：開放型システム間相互接続）階層モデルでの第２層以下にＡＴＭを使用し、第３および第４層にＴＣＰ／ＩＰプロトコルを使用するときの通信方式が、ＡＴＭ・フォーラム（The ATM Forum）等で審議されており、“ATM Forum 96－0824r9”等の仕様書が発表されている。“ATM Forum 96－0824r9”の仕様はＭＰＯＡ（Multiprotocol over ATM：マルチプロトコルを転送する仕組み）方式と呼ばれており、ＡＴＭネットワークインタフェースを持った端末やネットワークデバイスをＭＰＯＡクライアント（ＭＰＣ）とし、ルータ機能を有する装置をＭＰＯＡサーバ（ＭＰＳ）としてネットワークを構成する。

【０００５】ＭＰＣがＭＡＣフレームを転送するとき、送り先が同一サブネット内のＭＰＣまたはそのＭＰＣに収容される端末である場合には、ＡＴＭ・フォーラムが規定しているＬＡＮ（Local Area Network：企業情報通信網）エミュレーション（ＬＡＮＥ）プロトコルを用いて通信を行う。送り先が異なるサブネット内にあり、ＭＰＳ（ＭＰＯＡ方式のネットワーク内のサーバ）機能を持つルータにＭＡＣ（Media Access Control：媒体アクセス制御）フレーム内のＩＰアドレスを読み、そのＩＰアドレスごとにパケットをカウントするようにしている。得られたカウント値が単位時間内に一定値以下であれば、前記したＭＰＳにＭＡＣフレームを送信し、ＭＰＳは従来のルータと同じ動作で、ＩＰパケットを宛先のＩＰアドレスのノードまで送るようにする。

【０００６】これに対してカウント値が単位時間内に前記した一定値を越えた場合には、前記したＭＰＳにＭＡＣフレームを送信する代わりに、宛先ＩＰアドレスのノードと同一サブネットに存在するＭＰＣまでＶＣＣ（Virtual Channel Connection：仮想チャネル・コネクション）を設定し、そのＶＣＣを通してパケットを送る。これにより、ルータ（ＭＰＳ）をショートカットして、ＡＴＭの入口側のＭＰＣから、出口側のＭＰＣにＩＰパケットを送信することができる。したがって、前記したＶＣＣは、ショートカットＶＣＣと呼ばれている。ここでＡＴＭの入口側とは、他のネットワークからＭＰＯＡ（Multiprotocol Over ATM：ＡＴＭ上でマルチプロトコルを転送する仕組み）ネットワークにデータが流入するノードを表わしており、出口側とは、ＭＰＯＡネットワークから他のネットワークにデータが流出するノードを表わしている。

【０００７】ショートカットＶＣＣを設定するには、入

口側のＭＰＣがパケット内の受信先のＩＰアドレスから、出口側のＭＰＣのＡＴＭアドレスを得ることが必要である。このため、入口側ＭＰＣは、ＭＰＯＡレゾルーション・リクエスト（Resolution Request）を、同一サブネット内のＭＰＳに送出する。そして、ＭＰＳが出口側ＭＰＣと同じサブネットのときには、入口側ＭＰＣに対してＭＰＯＡレゾルーション・リプライ（Resolution Reply）で知らせ、出口側ＭＰＣに対してはＭＰＯＡインポジション・リクエスト（Imposition Request）を送る。また、ショートカットＶＣＣを通して送られてくるＭＡＣフレームを、出口側のＭＰＳから送られてきたように見せるために、出口側ＭＰＣでレイヤ２の情報を載せてＭＡＣフレームを送出する必要がある。このため、出口側ＭＰＳから出口側ＭＰＣに前記したＭＰＯＡインポジション・リクエスト・メッセージで通知を行う。ＭＰＳが出口側ＭＰＣとは異なるサブネットにあるときには、次段のＭＰＳにＭＰＯＡレゾルーション・リクエスト・メッセージを送ることになる。

【０００８】以上説明した手順で、入口側ＭＰＣが出口側のＭＰＣのＡＴＭアドレスを獲得したら、標準のＡＴＭのシグナリング手順（ＡＴＭ Forum UNI3.1 またはITU－TQ. 2931）を用いて、入口側ＭＰＣと出口側ＭＰＣの間にショートカットＶＣＣを設定する。そして以後、出口側ＭＰＣに送出する必要のあるデータは、このショートカットＶＣＣを通して送信することにしている。これにより、ＭＰＳにパケットを送信するよりも高速なデータ転送が可能になる。

【０００９】

【発明が解決しようとする課題】以上説明したようなＭＰＯＡ方式では、ショートカットＶＣＣを用いて送信されるＴＣＰ／ＵＤＰパケットが入口側ＭＰＣで４８バイトのセルに分割されてネットワークに送られる。そして、中継ＡＴＭ交換機をセルのままでスイッチングされて、出口側ＭＰＣで再びＴＣＰ／ＵＤＰパケットに組み立てられる。このため、ルータを使用した場合と異なって、中継のＡＴＭ交換機はパケット内のＴＣＰ／ＵＤＰヘッダやＩＰヘッダの読み込みを行わない。したがって、ＡＴＭ交換機を使用した場合には、ルータが従来行っていたトランスポート層レベルやネットワーク層レベルでのパケットのフィルタリングが不可能になるという問題があった。

【００１０】そこで本発明の目的は、ＭＰＯＡ方式のネットワークで、ルータと同様のパケットフィルタリング機能を実現することのできるパケットフィルタリングシステムを提供することにある。

【００１１】

【課題を解決するための手段】請求項１記載の発明では、非同期転送モードのＡＴＭネットワーク上に構築したマルチプロトコルの転送のためのＭＰＯＡネットワークで、送信側ＭＰＯＡクライアントがアドレス解決手順

を起動し、受信した受信ＩＰアドレスから出口側のＭＰＯＡ方式のネットワーク内のクライアントである出口側ＭＰＯＡクライアントのＡＴＭアドレスを獲得するようにした通信システムにおいて、（イ）アドレス解決要求メッセージを受信してこのメッセージ内の送受信ＩＰアドレスとＴＣＰまたはＵＤＰポート番号をそれぞれ読み込んでこれらをフィルタ用の情報としてのセット情報として、通常のデータ転送のために設定されたフィルタリングの基準に応じてアドレス解決要求に応じるか否かを判定する判定手段と、この判定手段の判定の結果としてアドレス解決要求に応じる場合にはアドレス解決手順を進行させ、アドレス解決要求に応じない場合にはアドレス解決を中止することで、複数のＭＰＯＡサーバ上のフィルタリング基準のすべてに適合するセット情報のパケットに対してのみアドレス解決の結果を返信する返信手段を備えたＭＰＯＡサーバと、（ロ）アドレス解決要求メッセージ内に、これから設定するショートカット仮想チャネル・コネクションとしてのショートカットＶＣＣを通して送信するパケットのセット情報を挿入する挿入手段と、アドレス解決要求時にセット情報のうちアドレス解決が中止されずに完了したもののみを記憶する第１の記憶手段と、パケット送信時にこの第１の記憶手段に記憶した内容と一致するＩＰパケットのみをショートカットＶＣＣに送信する送信手段と、アドレス解決要求時に、ＭＰＯＡサーバから通知されたショートカットＶＣＣを通して送信されてくるパケットのセット情報を記憶する第２の記憶手段と、パケット受信時にこの第２の記憶手段に記憶したセット情報と一致するＩＰパケットのみをショートカットＶＣＣから受けて、これ以外のＩＰパケットは廃棄するパケットフィルタリング手段とを備えたＭＰＯＡクライアントとをパケットフィルタリングシステムに具備させる。

【００１２】

【００１３】また、請求項２記載の発明では、ＡＴＭインタフェースと他のネットワークインタフェースを持ったデバイスとしてのエッジデバイスやＡＴＭ端末がトランスポート・コントロール・プロトコル／ユーザ・データグラム・プロトコルとしてのＴＣＰ／ＵＤＰヘッダとＩＰヘッダを読むことで、ＩＰアドレスとＴＣＰ／ＵＤＰポート番号によるパケットフィルタリングを実現することを特徴としている。

【００１４】すなわち本発明のパケットフィルタリングシステムでは、従来のルータと同様に、ＭＰＳにトランスポートレイヤとネットワークレイヤの情報によるフィルタリング規則を基にした基準を記述しておく。そして、入口側ＭＰＣが、ＡＴＭ交換機を用いたネットワーク上でＴＣＰ／ＩＰプロトコルによって通信を行う手法としてのＭＰＯＡプロトコルを使用して出口側ＭＰＣのＡＴＭアドレスを解決するときに、送信されるパケットの送信・受信ノードのＩＰアドレスと、トランスポート

層プロトコル（ＴＣＰまたはＵＤＰ）と、ＴＣＰ／ＵＤＰポート番号を申告し、それらが前記した基準によって禁止されていないかを中継のＭＰＳで検査する。この結果として禁止されていない場合には、アドレス解決手順が進められるが、禁止されていればアドレス解決手順を中止し、ショートカットＶＣＣを設定させないようにして、ＶＣＣ設定時のフィルタリングを実現する。

【００１５】これに加えて、ＶＣＣの設定後では、前記した入口側ＭＰＣがアドレス解決要求時に申告した属性を有するＴＣＰ／ＩＰパケットのみを送信し、それ以外のパケットはショートカットＶＣＣに送信しないようにして、データ送信時のフィルタリングを実現する。前記した出口側ＭＰＣでは、アドレス解決要求時に、入口側ＭＰＣから入口側ＭＰＳを通して申告された属性を有するＴＣＰ／ＩＰパケットのみを受け取り、それ以外のパケットを廃棄する。これにより、データ受信時のフィルタリングが実現される。

【００１６】

【発明の実施の形態】

【００１７】

【実施例】以下実施例につき本発明を詳細に説明する。

【００１８】本実施例のパケットフィルタリングシステムでは、異なるサブネットにあるＭＰＣ間でＩＰパケット通信を行うときに、ＩＰパケットのヘッダ内の送信・受信ノードのＩＰアドレスと、ＴＣＰ／ＵＤＰポート番号の双方によってフィルタリングを行うようにしている。ＭＰＣは、ＡＴＭインタフェースを持った端末の場合と、ＡＴＭインタフェースと他のネットワークインタフェースを持ったデバイス（これをエッジデバイスという。）の場合とがある。本実施例では後者のエッジデバイスの場合について説明を行う。また、実施例ではＩＰパケットヘッダ内の受信ノードのＩＰアドレスまたはＴＣＰ／ＵＤＰポート番号が異なるパケットでも、同一の入口側ＭＰＣと出口側ＭＰＣをとおるパケットは、同一のショートカットＶＣＣを使用する構成となっている。

【００１９】図１は本発明の一実施例におけるエッジデバイスの機能的な構成を表わしたものである。このエッジデバイスで、ＬＥＣ（LAN Emulation Client）処理部１１は、ＬＡＮＥＬ（LAN Emulation ）プロトコルを用いて、同一サブネット内のＬＥＣにＭＡＣフレームを転送するための処理を行う。ＬＥＣ処理部１１と接続されたＭＰＣ処理部１２は、ＭＰＯＡプロトコルを使用して、ＩＰパケットをカプセル化したＭＡＣフレームをＭＰＳと送受信したり、他のサブネット内のＭＰＣへのショートカットＶＣＣの設定のためのアドレス解決手順を行う。

【００２０】ＬＥＣ処理部１１およびＭＰＣ処理部１２に接続されたＶＣ（Virtual Circuit ）テーブル１３は、設定したＡＴＭのＶＣＣについての登録および管理を行う。ＡＴＭ　ＶＣ終端部１４は、図示しないＡＴＭネットワークとのインタフェースであり、ＡＴＭセルからパケットへの組み立てと、パケットからＡＴＭセルへの分解を行うようになっている。ＭＰＣ処理部１２に接続された非ＡＴＭネットワークインタフェース１５は、ＡＴＭ以外のネットワークとの入出力インタフェース部である。

【００２１】ＶＣテーブル１３およびＡＴＭ　ＶＣ終端部１４と接続されたＡＴＭシグナリング処理部１６は、ＡＴＭ　ＶＣＣを設定するためのシグナリングの制御と処理を行うようになっている。ＭＰＣ処理部１２と接続されたショートカットＶＣＣテーブル１７は、ＭＰＯＡプロトコルとＡＴＭシグナリングを用いて設定したショートカットＶＣＣ用のテーブルである。このショートカットＶＣＣテーブル１７の各ショートカットＶＣＣエントリには、そこを通過して送受信してもよいＴＣＰ／ＩＰパケットの属性が書かれるようになっている。

【００２２】図２は入口側ＭＰＣでのショートカットＶＣＣテーブルの例を示しており、図３は出口側ＭＰＣでのショートカットＶＣＣテーブルの例を示している。

【００２３】図４は、ＭＰＳの機能的な構成を表わしたものである。ＬＥＣ（ＬＡＮ Emulation Client ）処理部２１は、ＬＡＮＥ（ＬＡＮ Emulation）プロトコルを用いて、同一サブネット内のＬＥＣと通信を行う部分である。このＬＥＣ処理部２１と接続されたＭＰＳ処理部２２は、ＭＰＯＡプロトコルに基づいて、入力側ＭＰＣと出口側ＭＰＣに対してショートカットＶＣＣを設定するためのアドレス解決手順を制御する部分である。ルータ機能部２３は、他のＭＰＳや同一ネットワーク内のＭＰＣから送信されてきたＩＰパケットを、別のＭＰＳや他のサブネット内のＭＰＣに転送するためのルータとしての処理を行う。ＬＥＣ処理部２１、ＭＰＳ処理部２２およびルータ機能部２３と接続されたＶＣテーブル２４は、設定したＡＴＭのＶＣＣの登録や管理を行うようになっている。このＶＣテーブル２４に接続されたＡＴＭ　ＶＣ終端部２５は、図示しないＡＴＭネットワークとのインタフェースであり、ＡＴＭセルからパケットへの組み立てや、パケットからＡＴＭセルへの分解を行うようになっている。

【００２４】ＶＣテーブル２４およびＡＴＭ　ＶＣ終端部２５に接続されたＡＴＭシグナリング処理部２６は、ＡＴＭ　ＶＣＣを設定するためのシグナリングの制御と処理を行う。ＭＰＳ処理部２２およびルータ機能部２３と接続されたルーティング部２７は、他のサブネット内のＭＰＣやＭＰＳを探すためのルート検索テーブルである。このルート検索テーブルは、ルーティングプロトコルで動的に設定される場合と、管理者により静的に設定される場合とがある。ルート検索テーブル２７に接続されたＭＰＳパケットフィルタリング機能２８は、そのＭＰＳを通したＭＰＯＡプロトコルによるアドレス解決に制限を加え、ショートカットＶＣＣの設定を制限する部

分であり、管理者がこれを予め設定する。

【００２５】図５は、ＭＰＳパケットフィルタリング機能部の一例を示したものである。この図で列“１”は、ＩＰアドレスが“１１１．１１１．２２．２２”である送信端末のＴＣＰ“８０１０”番ポートと、ＩＰアドレスが“１１２．１１２．１２．１２”である受信端末のＴＣＰの２５番から１００番までのポートとの間に、ショートカットＶＣＣを設定してもよいことを示す。列“2”は、ＩＰアドレスが“１２２．１２２．２２．＊”であるネットワークに存在する送信端末のＵＤＰ（User Datagram Protocol）“５１７”番ポートを使用するアプリケーションＡＰ－１と、ＩＰアドレスが“１２２．１１２．１２．＊”のネットワークに存在する受信端末のＵＤＰ“８０８０”番ポートを使用するアプリケーションＡＰ－１との間に、ショートカットＶＣＣを設定してもよいことを示す。

【００２６】この図５に示すように、送信ＩＰアドレス（またはそのプレフィックス）と受信ＩＰアドレス（またはそのプレフィックス）の組で１つのエントリが構成され、かつここでアドレスの解決が禁止されていない場合のみ、アドレス解決未処理の回答要求を行うようになっている。

【００２７】図６は、入口側ＭＰＣが、ＡＴＭ以外のネットワークから受けたＭＡＣフレームを中継するときの処理の流れを表わしたものである。まず、入口側ＭＰＣは、受信したＭＡＣフレーム　内の受信先ＭＡＣアドレスと受信先ＩＰアドレスを読み出す（ステップＳ１０１）。そして、受信先ＭＡＣアドレスが同一サブネット内のＭＰＳであるか否かを判別する（ステップＳ１０２）。受信先ＭＡＣアドレスが同一サブネット内のＭＰＳ以外である場合には（Ｙ）、ＬＡＮＥプロトコルを用いて、受信先のノードにＭＡＣフレームを送る（ステップＳ１０３）。

【００２８】これに対して、受信先ＭＡＣアドレスが同一サブネット内のＭＰＳである場合（ステップＳ１０２：Ｎ）、受信先ＩＰアドレスを鍵として、ショートカットＶＣＣテーブル１７内のショートカットＶＣＣのエントリを検索する（ステップＳ１０４）。この鍵に対するエントリが見つからない場合には（ステップＳ１０５：Ｎ）、新たにエントリを作成し、そのカウンタのカウント値を“１“に設定して、受信したＭＡＣフレームを入口側ＭＰＳに送る（ステップＳ１０６）。この鍵に対応するエントリが見つかった場合には（ステップＳ１０５：Ｙ）、ショートカットＶＣＣが未設定であるかどうかを判別する（ステップＳ１０７）。

【００２９】図７は、鍵に対応するエントリが見つかったがそのショートカットＶＣＣが未設定の場合の処理手順を表わしたものである。この場合には、まずカウント値を“１“加算する（ステップＳ２０１）。そして、ショートカットＶＣＣエントリのカウント値とあらかじめ

設定されたしきい値とを比較する（ステップＳ２０２）。この結果、しきい値の方が大きいときには（ステップＳ２０３：Ｙ）、入口側ＭＰＳにＭＡＣフレームを送信して処理を終える（エンド）。カウント値の方が大きいか両者が等しい場合には、ＭＡＣフレームの中のＩＰパケットヘッダ内の送受信ＩＰアドレスと、ＴＣＰ／ＵＤＰポート番号を読み、そのパケットを入口側ＭＰＳに送る（ステップＳ２０４）。次に、出口側ＭＰＣのＡＴＭアドレスを得るために、ＭＰＯＡレゾルーション・リクエスト・メッセージを同一サブネット内のＭＰＳ（入口側ＭＰＳ）に送信する（ステップＳ２０５）。このメッセージに、標準のＭＰＯＡプロトコルで規定される情報を加えて、ステップＳ２０４で読み出したＩＰパケットの送受信ＩＰアドレスとＴＣＰ／ＵＤＰポート番号を含める。このＭＰＯＡレゾルーション・リクエストが成功すると、次の手順として入口側ＭＰＳからＭＰＯＡレゾルーション・リプライが戻り、出口側ＭＰＣのＡＴＭアドレスが通知される（ステップＳ２０６）。

【００３０】次に、前記したエントリに、出口側ＭＰＣのＡＴＭアドレスと、送信するＴＣＰ／ＩＰパケットの送信・受信ＩＰアドレスと、ＴＣＰ／ＵＤＰポート番号を登録する（ステップＳ２０７）。そして、出口側ＭＰＣのＡＴＭアドレスを宛先として、標準のＡＴＭシグナリング手順を行って、ショートカットＶＣＣを設定する（ステップＳ２０８）。その後、ステップＳ２０８で設定したショートカットＶＣＣのＶＰＩ／ＶＣＩ（Virtual Path identifier ／Virtual Channel identifier；仮想パス識別子／仮想チャネル識別子）を、前記したショートカットＶＣＣのエントリに設定する（ステップＳ２０９）。

【００３１】図８は、図６のステップＳ１０７で鍵に対応するエントリが見つかり、ショートカットＶＣＣが設定済である場合の処理の流れを表わしたものである。この場合には、まずＭＡＣフレーム中のＩＰパケットヘッダの送信・受信ＩＰアドレスとＴＣＰ／ＵＤＰポート番号を読み出す（ステップＳ３０１）。そして、出口側ＭＰＣへのショートカットＶＣＣが設定されているので、この設定されているショートカットＶＣＣエントリ中の送信・受信ＩＰアドレスおよびＴＣＰ／ＵＤＰポート番号を、ステップＳ３０１で読んだＩＰパケット内の送信・受信ＩＰアドレスおよびＴＣＰ／ＵＤＰポート番号とそれぞれ比較する（ステップＳ３０２）。これらの値がどれも一致している場合には（ステップＳ３０３：Ｙ）、前記したエントリの出口側ＭＰＣへのショートカットＶＣＣに、受信したＭＡＣフレームを送信する（ステップＳ３０４）。

【００３２】これらの値のいずれかが等しくない場合には（ステップＳ３０３：Ｎ）、入口側のＭＰＳに対してＭＰＯＡレゾルーション・リクエストを送信し、受信したＭＡＣフレームを入口側ＭＰＳに送る（ステップＳ３

０５）。このメッセージに、標準のＭＰＯＡプロトコルで規定される所と共に、ステップＳ３０１で読み出したＩＰパケットの送受信ＩＰアドレスとＴＣＰ／ＵＤＰポート番号とを含める。このＭＰＯＡレゾルーション・リクエストが成功して、ＭＰＳからＭＰＯＡレゾルーション・リプライが戻ってきた場合には（ステップＳ３０６：Ｙ）、出口側ＭＰＣのＡＴＭアドレスが通知され、前記したＩＰパケットの送信が許可されたことになる。したがって、このときには、前記したエントリに、新たに送信するＴＣＰ／ＩＰパケットの送信・受信アドレスと、ＴＣＰ／ＵＤＰポート番号を追加登録する（ステップＳ３０７）。

【００３３】ステップＳ３０６でＭＰＳからＭＰＯＡレゾルーション・リプライが戻ってこない場合には（Ｎ）、前記したＩＰパケットをショートカットＶＣＣを通して送信することが許可されないことになり、処理を終える（エンド）。

【００３４】図９は、ＭＰＳが、入口側のＭＰＣからＭＰＯＡレゾルーション・リクエスト・メッセージを受けるときの処理の流れを表わしたものである。まず図４に示したＭＰＳ処理部２２は、隣接したＭＰＣからＭＰＯＡレゾルーション・リクエスト・メッセージを受信する（ステップＳ４０１）。次に、そのメッセージ中の送信・受信ＩＰアドレスとＴＣＰ／ＵＤＰポート番号を読む（ステップＳ４０２）。そして、ＭＰＳパケットフィルタリング機能部２８（図４）を検索して、そのパケットをショートカットＶＣＣを通して受信するために、アドレス解決をしてよいかの判定処理を行う（ステップＳ４０３）。この結果、解決が許可されていない時には（ステップＳ４０４：Ｙ）、そのＭＰＯＡレゾルーション・リクエスト・メッセージを廃棄し、入力側ＭＰＣと出力側ＭＰＣにショートカットＶＣＣを設定するのを中断させる（ステップＳ４０５）。

【００３５】これに対して、ステップＳ４０４で解決が許可されているときには（Ｎ）、受信先ＩＰアドレスから、ルーティング部２７を用いて、出口側ＭＰＣへのルートを検索する（ステップＳ４０６）。出口側ＭＰＣがこのＭＰＳと異なるサブネットに存在する時には、（ステップＳ４０７：Ｙ）、次段のＮＨＲＰ（Next Hop Resolution Protocol）サーバに前記したＭＰＯＡレゾルーション・リクエスト・メッセージを転送する（ステップＳ４０８）。ステップＳ４０７で出口側ＭＰＣが同一サブネットに存在するときには（Ｎ）、出口側ＭＰＣに対して、ＭＰＯＡキャッシ・インポジション（Cache Imposition）・メッセージを送信する（ステップＳ４０９）。このメッセージの中には、標準のＭＰＯＡプロトコルで規定されている、このＭＰＳのＭＡＣアドレスと、受信先のＩＰノードのＭＡＣアドレスおよび受信先のＩＰアドレスに加えて、そのショートカットＶＣＣを通して送られるパケットの送信ＩＰアドレスと送受信のＴＣＰ／ＵＤＰポート番号とが含まれる。次に入口側ＭＰＣに対して、ＭＰＯＡレゾルーション・リプライ（Resolution Reply）メッセージを送る。

【００３６】図１０は、ＭＰＣが、ショートカットＶＣＣを設定するために、出口側ＭＰＳからＭＰＯＡキャッシ・インポジション・メッセージを受信する場合の処理の流れを表わしたものである。まず、ＭＰＯＡキャッシ・インポジション・メッセージを受信する（ステップＳ５０１）。次にこのＭＰＯＡキャッシ・インポジション・メッセージから、標準のＭＰＯＡプロトコルで規定されている入口側ＭＰＣのＡＴＭアドレスと、出口側ＭＰＳのＭＡＣアドレスと、受信ＩＰノードのＭＡＣアドレスに加えて、送信されるＩＰパケットの受信ＩＰアドレスと、送受信のＴＣＰ／ＩＤＰポート番号を読み取る（ステップＳ５０２）。

【００３７】次に、入口側ＭＰＣのＡＴＭアドレスと、受信ＩＰノードのＩＰアドレスを鍵として、ショートカットＶＣＣテーブル１７（図１）にエントリを検索する（ステップＳ５０３）。エントリがない場合には（ステップＳ５０４：Ｙ）、ステップＳ５０２で読み出した、送信されるＴＣＰ／ＩＰパケットの送受信ＩＰアドレスと、ＴＣＰ／ＩＤＰポート番号と、入口側ＭＰＣのＡＴＭアドレスと、出口側ＭＰＳのＭＡＣアドレスおよび受信ＩＰノードのＭＡＣアドレスを、ショートカットＶＣＣテーブル１７に登録する（ステップＳ５０５）。その後、ＡＴＭシグナリング手順によってショートカットＶＣＣのＶＰＩ／ＶＣＩが決定されるので、その値を前記したエントリに登録する（ステップＳ５０６）。

【００３８】ステップＳ５０４でエントリが既に存在する場合には、ステップＳ５０２で読み出した、送信されるパケットの送信ＩＰアドレスと、送信・受信ＴＣＰ／ＩＤＰポート番号をこのエントリに追加登録する（ステップＳ５０６）。

【００３９】図１１は、出口側ＭＰＣが、ショートカットＶＣＣを通してパケットを受信するときの処理の流れを表わしたものである。まず、ショートカットＶＣＣを通して、セル化されたＩＰパケットを受信する（ステップＳ６０１）。次に、図１に示したＡＴＭ　ＶＣ終端部１４でセルからＩＰパケットを組み立てる（ステップＳ６０２）。そして、出口側ショートカットＶＣＣテーブル１７（図１）内で、パケットが送られてきたショートカットＶＣＣのＶＰＩ／ＶＣＩと受信先ＩＰアドレスを鍵として、該当するエントリを検索する（ステップＳ６０３）。次に、受信したＩＰパケット内の送信・受信ＩＰアドレスとＴＣＰ／ＵＤＰポート番号を読み出す（ステップＳ６０４）。そして、ステップＳ６０４で読んだ値と前記したショートカットＶＣＣの該当エントリの送信・受信ＩＰアドレスとＴＣＰ／ＵＤＰポート番号とを比較する（ステップＳ６０５）。

【００４０】この結果としていずれも等しいときには

（ステップＳ６０６：Ｙ）、許可されたパケットであるとして、同一サブネット内のＭＰＳのＭＡＣアドレスと、受信先のＩＰノードのＭＡＣアドレスを付加してＭＡＣフレームとし、非ＡＴＭインタフェース１５（図１）から該当するネットワークに送信する（ステップＳ６０７）。ステップＳ６０６でいずれかが等しくない場合には（Ｎ）、違反パケットであるとみなしてこれを廃棄し、パケットフィルタリングを実行することになる（ステップＳ６０８）。

【００４１】

【発明の効果】以上説明したように請求項１～請求項２記載の発明によれば、ＴＣＰ／ＵＤＰパケットごとにＡＴＭ交換機でＴＣＰ／ＵＤＰヘッダとＩＰヘッダを読まなくとも、エッジデバイスやＡＴＭ端末でそれらのヘッダを読むことで、ＩＰアドレスとＴＣＰ／ＵＤＰポート番号によるパケットフィルタリングを実現することができる。本発明では、あらかじめフィルタリングの基準を設定しておくので、たとえば、これをＭＰＳ機能を持ったルータで設定した実施例の図５で示したような基準とすれば、これがＭＰＯＡプロトコルのメッセージと共に、エッジデバイスやＡＴＭ端末に伝播する。したがって、ＭＰＳ機能を持ったルータに適切なフィルタリング規則の内容を設定しておくと、その下流側に存在するすべてのＩＰノードの通信の安全性が向上するという利点がある。しかも本発明では、単にフィルタ条件を判定してその結果がクライアントに返されるのではなく、それぞれのサーバを通過可能なときにはこれらによるアドレス解決手順が続行されるので、フィルタ条件を重畳させた形でクライアントが取得するという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例におけるエッジデバイスの機能的な構成を示すブロック図である。

【図２】本実施例の入口側ＭＰＣでのショートカットＶＣＣテーブルの内容を示した説明図である。

【図３】本実施例の出口側ＭＰＣでのショートカットＶＣＣテーブルの内容を示した説明図である。

【図４】本実施例のＭＰＳの機能的な構成を表わしたブロック図である。

【図５】ＭＰＳパケットフィルタリング機能部の一例を示した説明図である。

【図６】入口側ＭＰＣが、ＡＴＭ以外のネットワークから受けたＭＡＣフレームを中継するときの処理の流れを表わした流れ図である。

【図７】鍵に対応するエントリが見つかったがそのショートカットＶＣＣが未設定の場合の処理手順を表わした流れ図である。

【図８】図６のステップＳ１０７で鍵に対応するエントリが見つかり、ショートカットＶＣＣが設定済である場合の処理の流れを表わした流れ図である。

【図９】ＭＰＳが、入口側のＭＰＣからＭＰＯＡレゾルーション・リクエスト・メッセージを受けるときの処理の流れを表わした流れ図である。

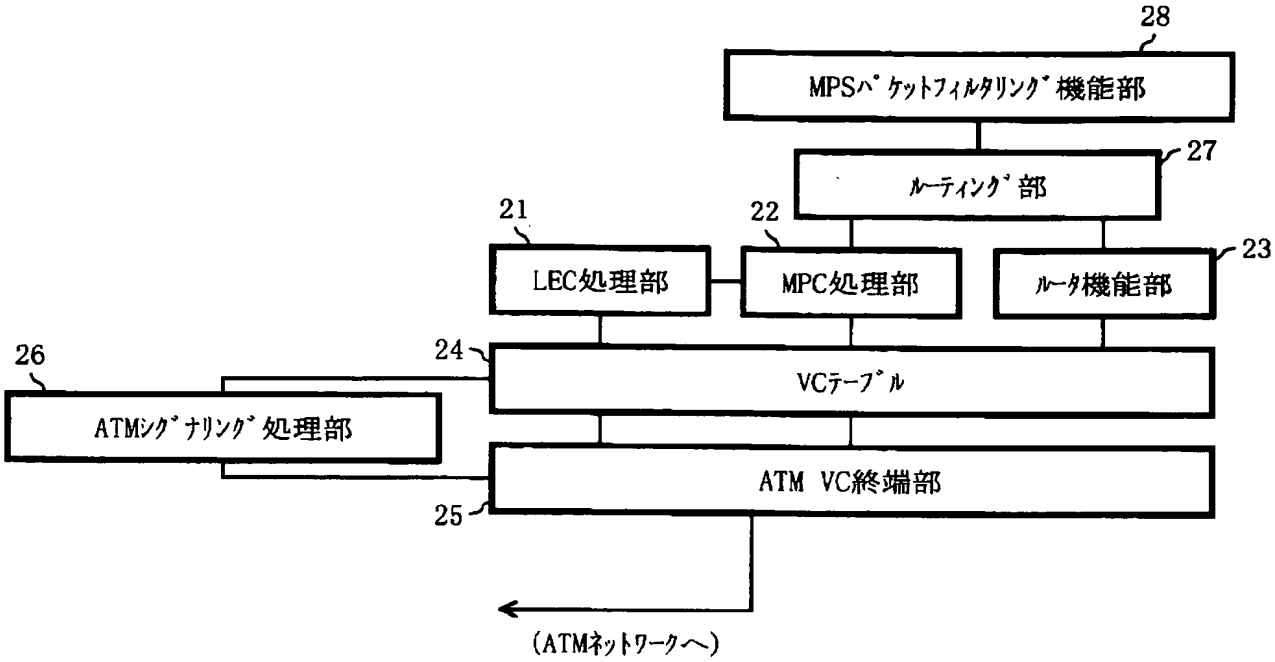
【図１０】ＭＰＣが、ショートカットＶＣＣを設定するために、出口側ＭＰＳからＭＰＯＡキャッシ・インポジション・メッセージを受信する場合の処理の流れを表わした流れ図である。

【図１１】出口側ＭＰＣが、ショートカットＶＣＣを通してパケットを受信するときの処理の流れを表わした流れ図である。

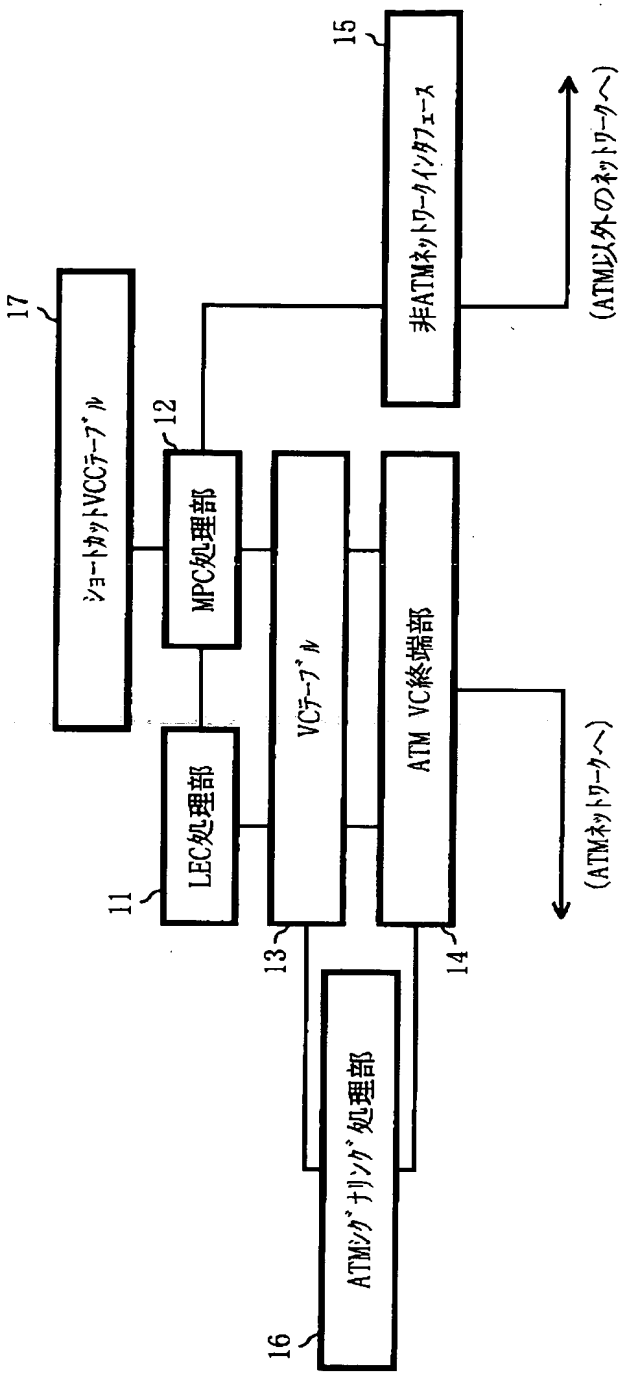
【符号の説明】

１１、２１　ＬＥＣ処理部
１２　ＭＰＣ処理部
１３、２２、２４　ＶＣテーブル
１４、２５　ＡＴＭ　ＶＣ終端部
１５　非ＡＴＭネットワークインターフェース部
１６、２６　ＡＴＭシグナリング処理部
１７　ショートカットＶＣＣテーブル
２３　ルータ機能部
２７　ルーティング部
２８　ＭＰＳパケットフィルタリング機能部

【図４】


28
MPSﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ機能部
27
ﾙｰﾃｨﾝｸﾞ部
21
22
23
LEC処理部
MPC処理部
ﾙｰﾀ機能部
26
24
VCﾃｰﾌﾞﾙ
ATMｼﾝｸﾞﾅﾘﾝｸﾞ処理部
ATM VC終端部
25
(ATMﾈｯﾄﾜｰｸへ)

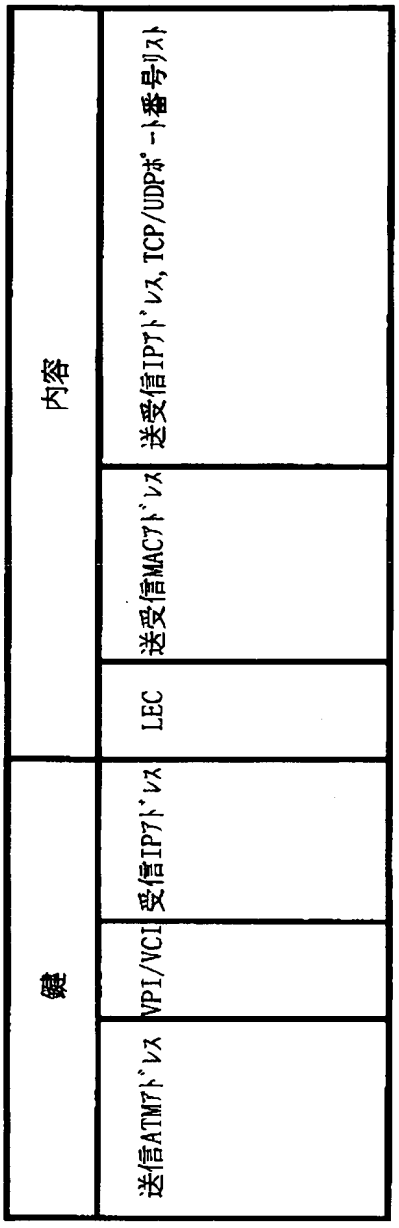
【図１】



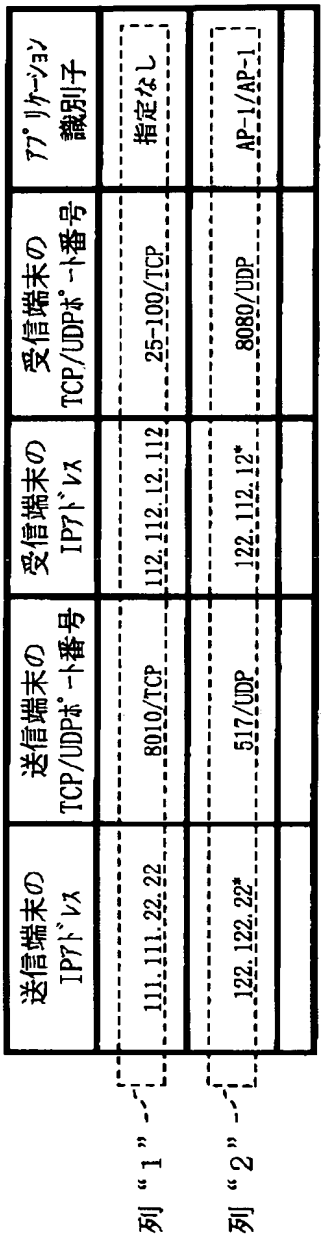
【図２】

鍵		内容
LEC番号		
受信MACアドレス		
受信IPアドレス		
カウンタ		
受信ATMアドレス		
VPI/VCI		
送受信IPアドレス, TCP/UDPポート番号リスト		

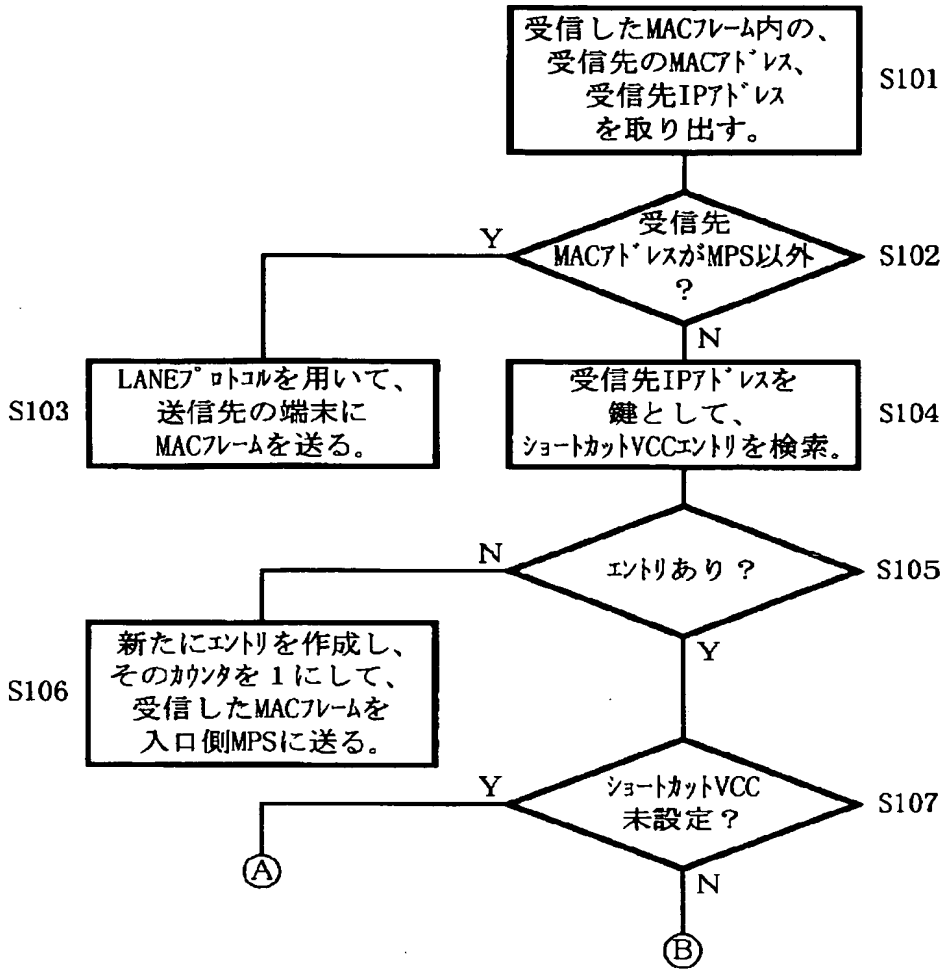
【図３】


鍵
内容
送信ATMｱﾄﾞﾚｽ
VPI/VCI
受信IPｱﾄﾞﾚｽ
LEC
送受信MACｱﾄﾞﾚｽ
送受信IPｱﾄﾞﾚｽ, TCP/UDPﾎﾟｰﾄ番号ﾘｽﾄ

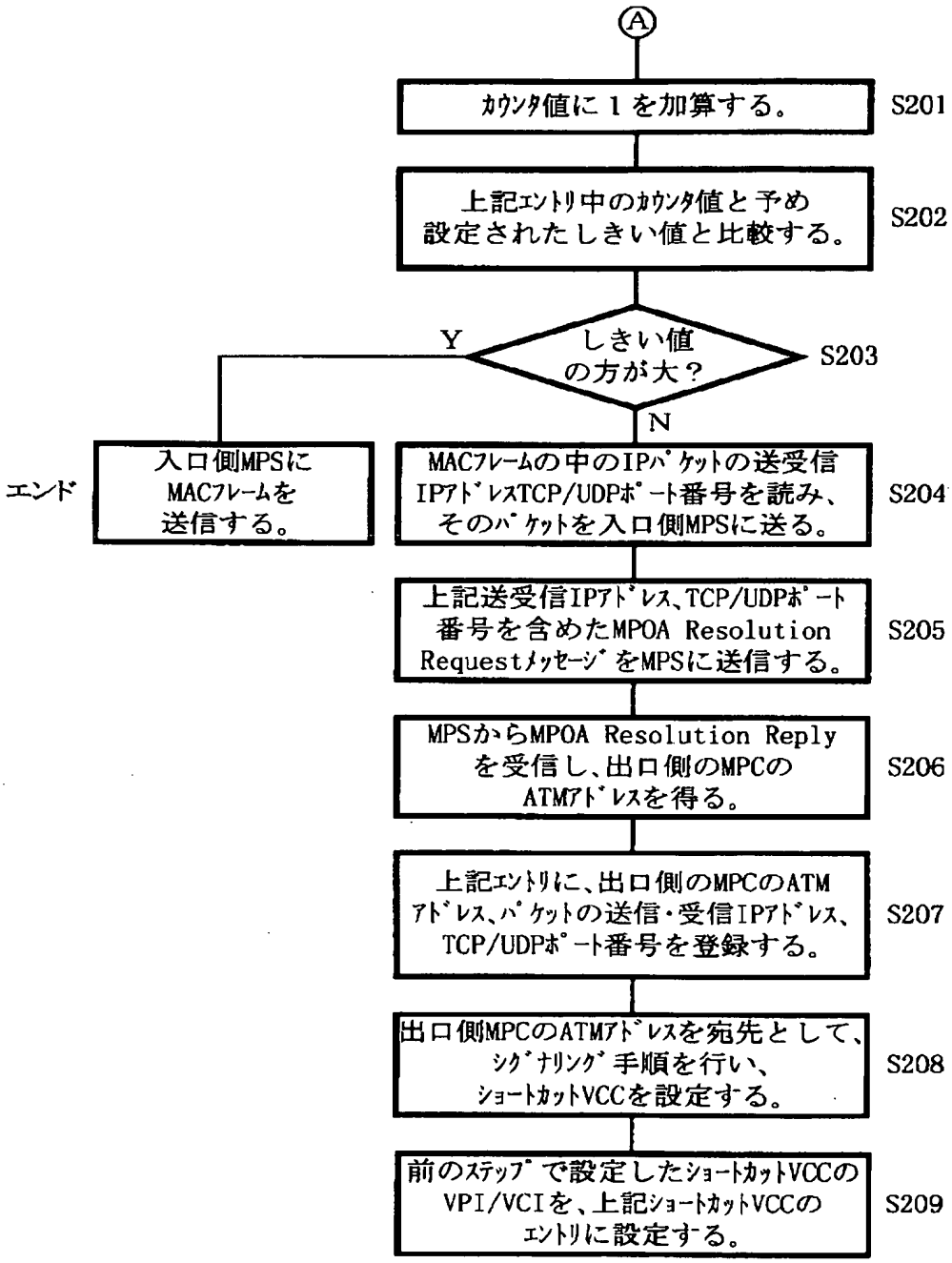
【図５】


送信端末のIPｱﾄﾞﾚｽ
送信端末のTCP/UDPﾎﾟｰﾄ番号
受信端末のIPｱﾄﾞﾚｽ
受信端末のTCP/UDPﾎﾟｰﾄ番号
ｱﾌﾟﾘｹｰｼｮﾝ識別子
列“1”
111.111.22.22
8010/TCP
112.112.12.112
25-100/TCP
指定なし
列“2”
122.122.22*
517/UDP
122.112.12*
8080/UDP
AP-1/AP-1

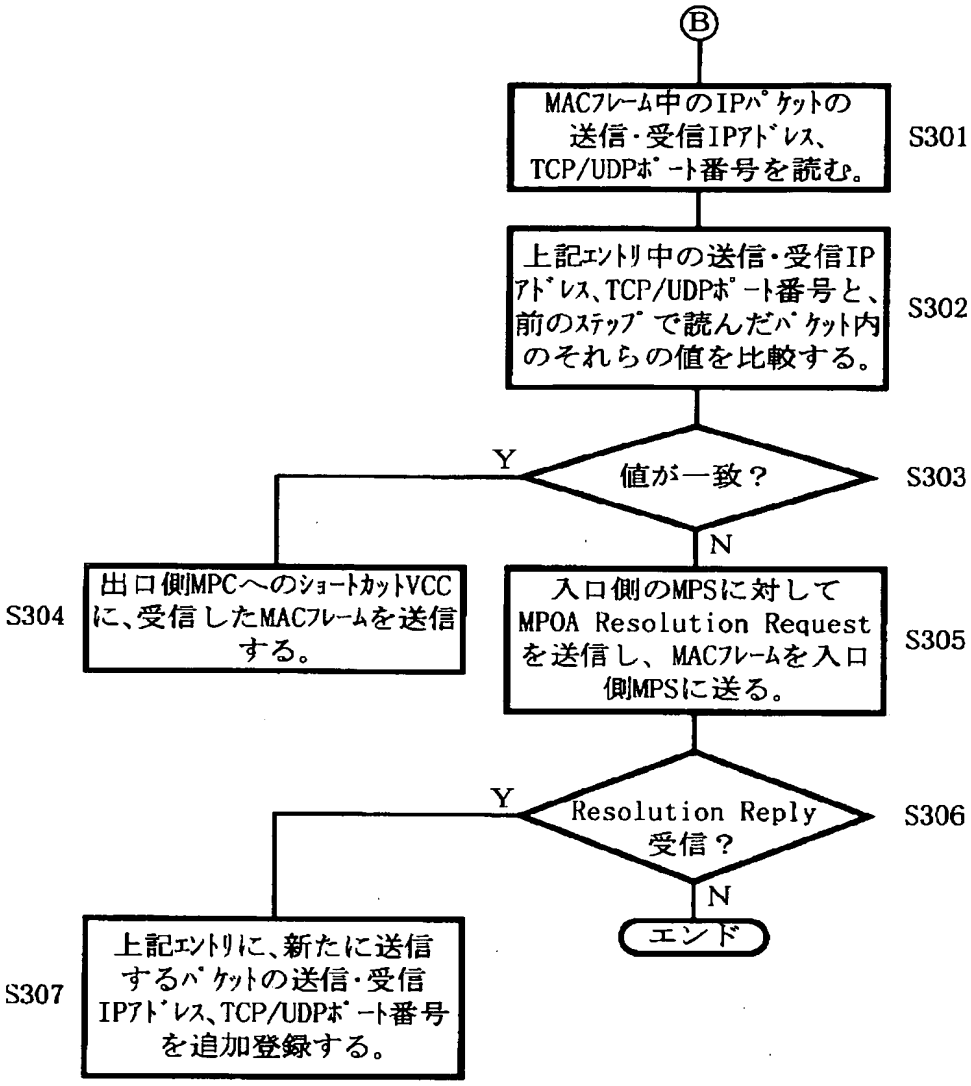
【図６】


受信したMACフレーム内の、受信先のMACアドレス、受信先IPアドレスを取り出す。
S101
受信先MACアドレスがMPS以外？
S102
Y
N
LANEプロトコルを用いて、送信先の端末にMACフレームを送る。
S103
受信先IPアドレスを鍵として、ショートカットVCCエントリを検索。
S104
エントリあり？
S105
N
Y
新たにエントリを作成し、そのカウンタを１にして、受信したMACフレームを入口側MPSに送る。
S106
ショートカットVCC未設定？
S107
Y
N
Ⓐ
Ⓑ

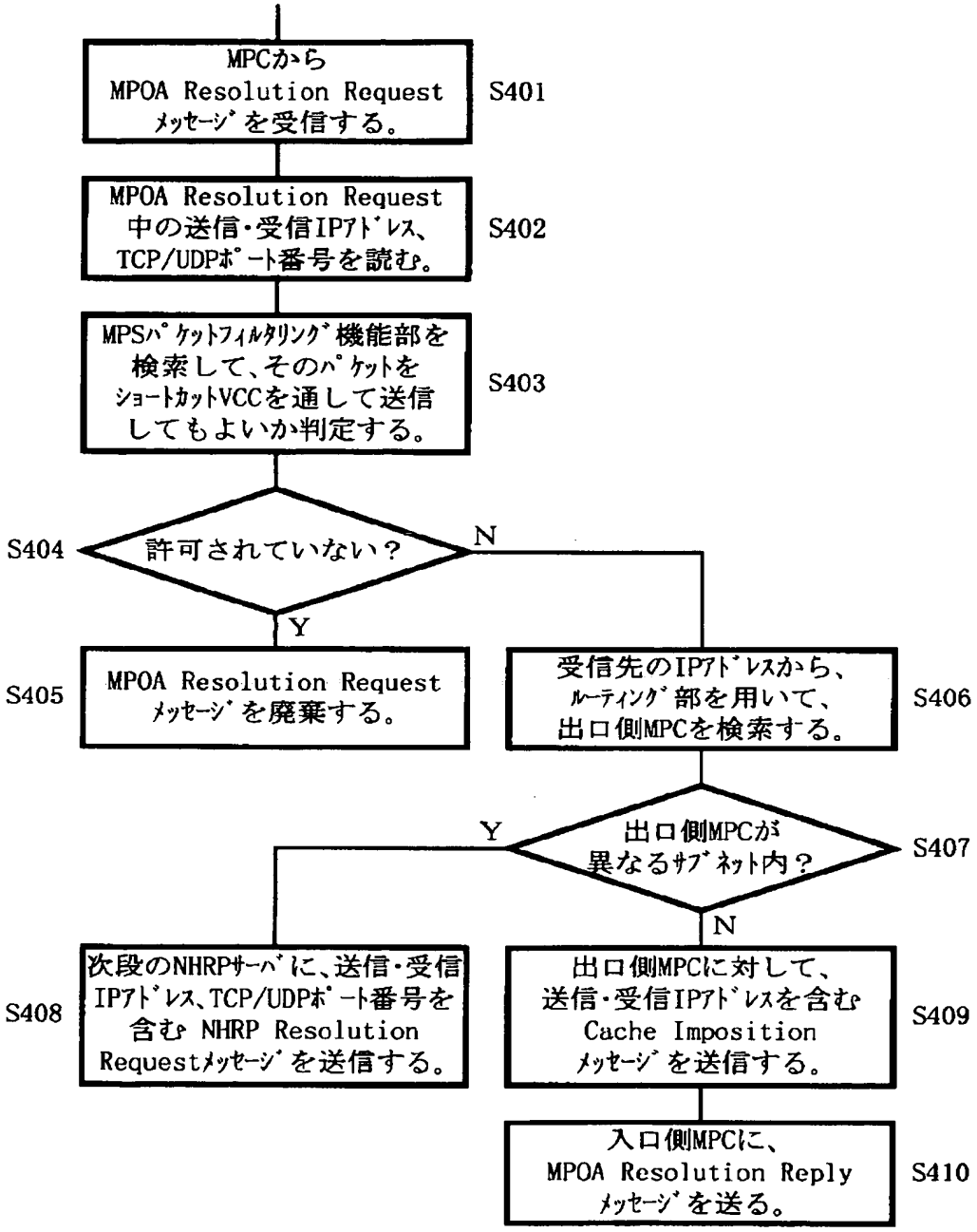
【図７】


A
カウンタ値に１を加算する。
S201
上記エントリ中のカウンタ値と予め設定されたしきい値と比較する。
S202
しきい値の方が大？
S203
Y
N
エンド
入口側MPSにMACフレームを送信する。
MACフレームの中のIPパケットの送受信IPアドレスTCP/UDPポート番号を読み、そのパケットを入口側MPSに送る。
S204
上記送受信IPアドレス、TCP/UDPポート番号を含めたMPOA Resolution Requestメッセージ をMPSに送信する。
S205
MPSからMPOA Resolution Replyを受信し、出口側のMPCのATMアドレスを得る。
S206
上記エントリに、出口側のMPCのATMアドレス、パケットの送信・受信IPアドレス、TCP/UDPポート番号を登録する。
S207
出口側MPCのATMアドレスを宛先として、シグナリング手順を行い、ショートカットVCCを設定する。
S208
前のステップで設定したショートカットVCCのVPI/VCIを、上記ショートカットVCCのエントリに設定する。
S209

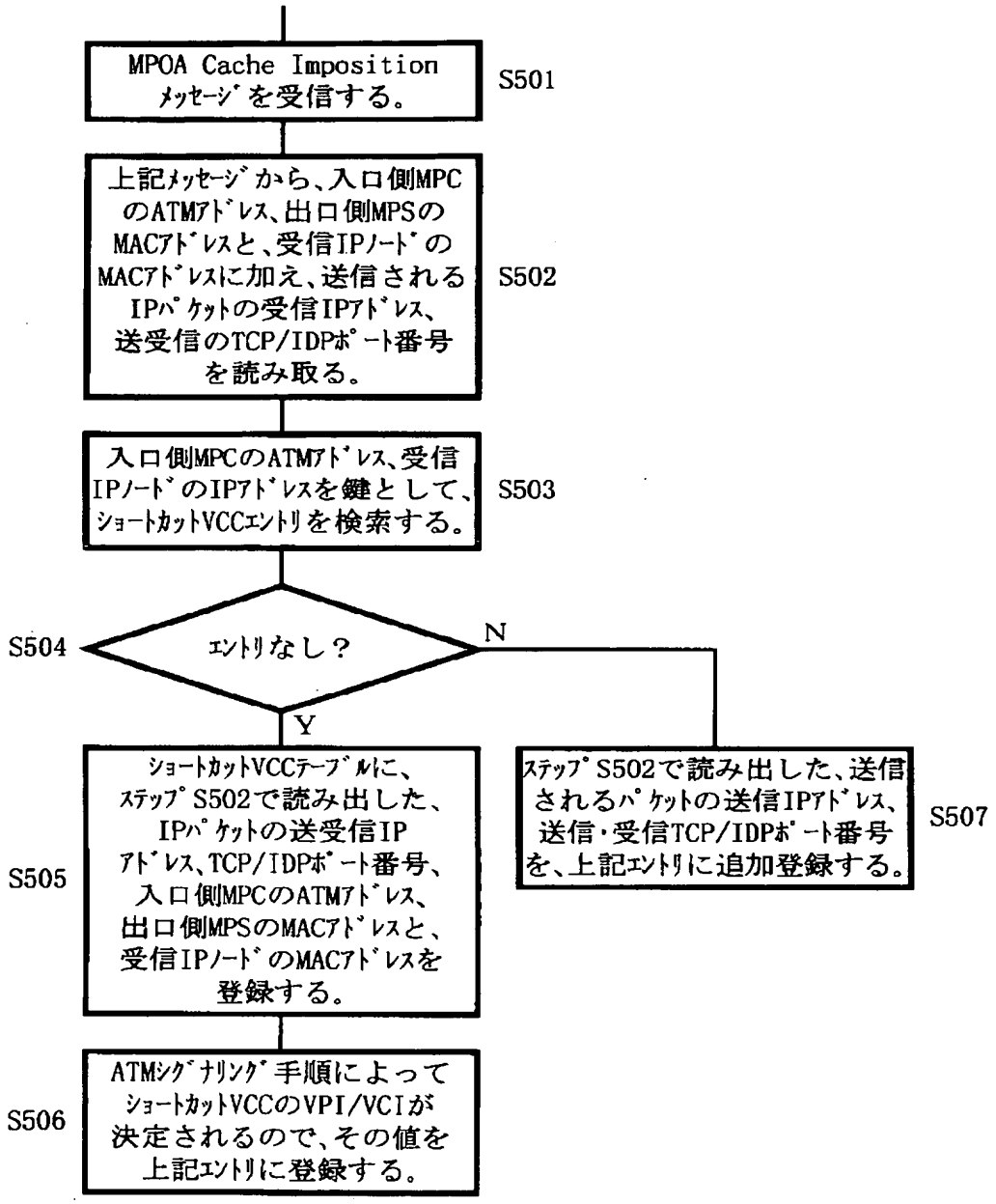
【図８】


Ⓑ
MACフレーム中のIPパケットの送信・受信IPアドレス、TCP/UDPポート番号を読む。
S301
上記エントリ中の送信・受信IPアドレス、TCP/UDPポート番号と、前のステップで読んだパケット内のそれらの値を比較する。
S302
値が一致？
S303
Y
N
出口側MPCへのショートカットVCCに、受信したMACフレームを送信する。
S304
入口側のMPSに対してMPOA Resolution Requestを送信し、MACフレームを入口側MPSに送る。
S305
Resolution Reply受信？
S306
Y
N
エンド
上記エントリに、新たに送信するパケットの送信・受信IPアドレス、TCP/UDPポート番号を追加登録する。
S307

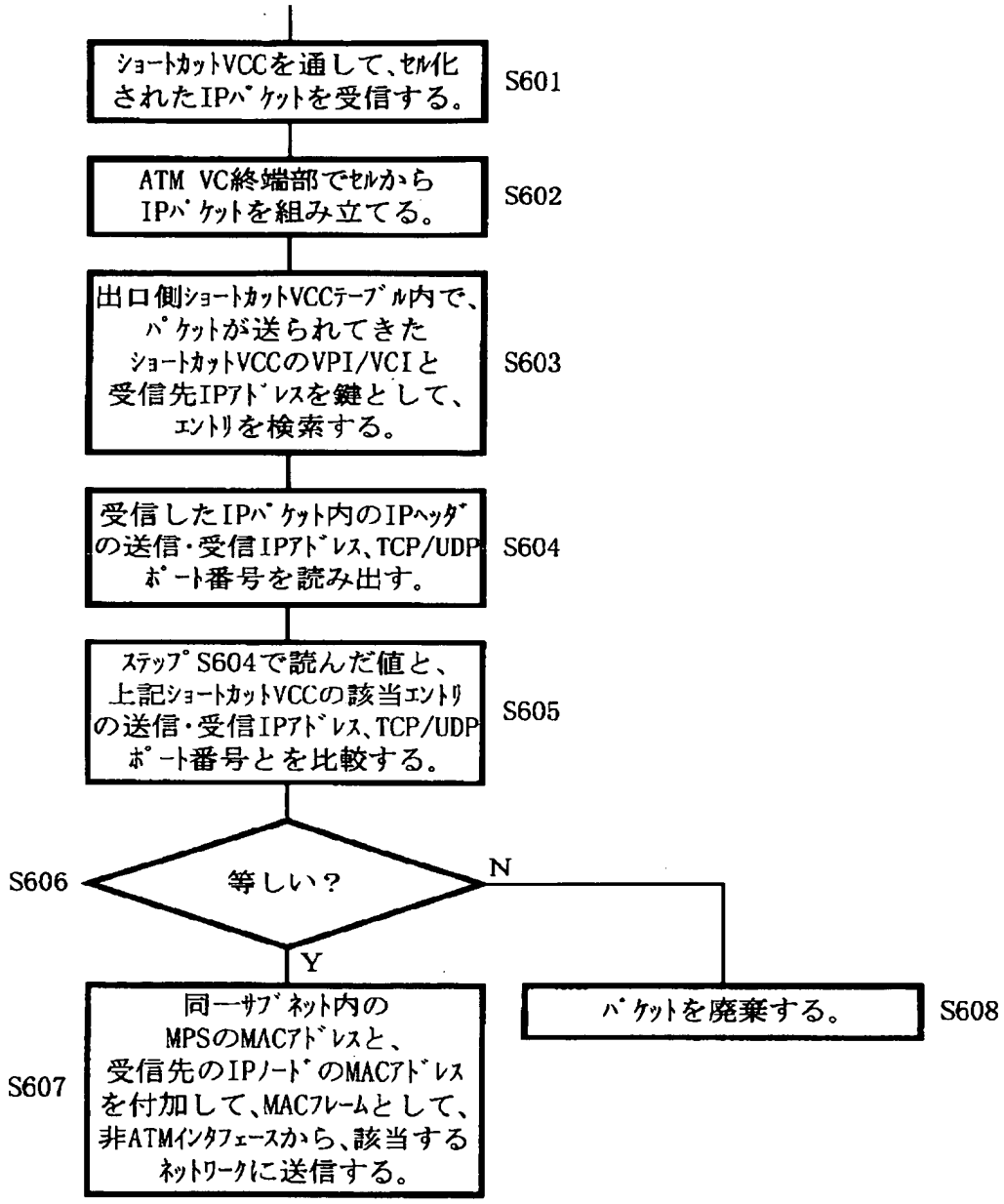
【図９】


MPCから
MPOA Resolution Request
ﾒｯｾｰｼﾞを受信する。
S401
MPOA Resolution Request
中の送信・受信IPｱﾄﾞﾚｽ、
TCP/UDPﾎﾟｰﾄ番号を読む。
S402
MPSﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ機能部を
検索して、そのﾊﾟｹｯﾄを
ｼｮｰﾄｶｯﾄVCCを通して送信
してもよいか判定する。
S403
S404
許可されていない？
N
Y
S405
MPOA Resolution Request
ﾒｯｾｰｼﾞを廃棄する。
受信先のIPｱﾄﾞﾚｽから、
ﾙｰﾃｨﾝｸﾞ部を用いて、
出口側MPCを検索する。
S406
Y
出口側MPCが
異なるｻﾌﾞﾈｯﾄ内？
S407
N
S408
次段のNHRPｻｰﾊﾞに、送信・受信
IPｱﾄﾞﾚｽ、TCP/UDPﾎﾟｰﾄ番号を
含む NHRP Resolution
Requestﾒｯｾｰｼﾞを送信する。
出口側MPCに対して、
送信・受信IPｱﾄﾞﾚｽを含む
Cache Imposition
ﾒｯｾｰｼﾞを送信する。
S409
入口側MPCに、
MPOA Resolution Reply
ﾒｯｾｰｼﾞを送る。
S410

【図１０】


MPOA Cache Imposition メッセージを受信する。
S501
上記メッセージから、入口側MPCのATMアドレス、出口側MPSのMACアドレスと、受信IPノードのMACアドレスに加え、送信されるIPパケットの受信IPアドレス、送受信のTCP/IDPポート番号を読み取る。
S502
入口側MPCのATMアドレス、受信IPノードのIPアドレスを鍵として、ショートカットVCCエントリを検索する。
S503
S504
エントリなし？
N
Y
ショートカットVCCテーブルに、ステップS502で読み出した、IPパケットの送受信IPアドレス、TCP/IDPポート番号、入口側MPCのATMアドレス、出口側MPSのMACアドレスと、受信IPノードのMACアドレスを登録する。
S505
ATMシグナリング手順によってショートカットVCCのVPI/VCIが決定されるので、その値を上記エントリに登録する。
S506
ステップS502で読み出した、送信されるパケットの送信IPアドレス、送信・受信TCP/IDPポート番号を、上記エントリに追加登録する。
S507

【図１１】


ショートカットVCCを通して、セル化されたIPパケットを受信する。
S601
ATM VC終端部でセルからIPパケットを組み立てる。
S602
出口側ショートカットVCCテーブル内で、パケットが送られてきたショートカットVCCのVPI/VCIと受信先IPアドレスを鍵として、エントリを検索する。
S603
受信したIPパケット内のIPヘッダの送信・受信IPアドレス、TCP/UDPポート番号を読み出す。
S604
ステップS604で読んだ値と、上記ショートカットVCCの該当エントリの送信・受信IPアドレス、TCP/UDPポート番号とを比較する。
S605
S606
等しい？
N
Y
同一サブネット内のMPSのMACアドレスと、受信先のIPノードのMACアドレスを付加して、MACフレームとして、非ATMインタフェースから、該当するネットワークに送信する。
S607
パケットを廃棄する。
S608